UNIVERSITÉ DE MONTRÉAL

CENTRE DE RECHERCHE SUR LES TRANSPORTS

CASE POSTALE 6128, SUCCURSALE A, MONTREAL, QUEBEC, H3C 3J7

EXTRACTION DE RELATIONS LOGIQUES ET SAUT DE DUALITÉ

par

Brigitte Jaumard* et François Soumis**

* RUTCOR et CAIP, Rutgers University, New Brunswick, NJ 08903, U.S.A.

** École Polytechnique de Montréal, C.P. 6079, Succursale A, Montréal, CANADA H3C 3A7.

Cette étude a été publiée grâce à une subvention du fonds F.C.A.R. pour l'aide et le soutien à la recherche.

Université de Montréal
Centre de recherche sur les transports - Publication #458-F
Avril 1986

Dépôt légal - 4e trimestre 1986

RÉSUMÉ

Ce papier s'intéresse à la détermination des variables à valeur fixe dans les systèmes de contraintes linéaires en variables 0-1. On rappelle tout d'abord la méthode d'extraction des relations logiques développée par Jaumard et Minoux pour un système de contraintes linéaires en variables 0-1. Dans le cas particulier de l'identification de variables à valeur fixe, on montre que l'efficacité de la méthode dépend du saut de dualité d'un problème d'optimisation défini à partir du système de contraintes. On illustre les propriétés obtenues sur un problème de décodage de vote qui se formule soit comme une extension du problème d'affectation généralisé soit comme un problème de partitionnement. On montre que, suivant la formulation retenue, le nombre de variables à valeur fixe identifiées varie et que les différences obtenues s'expliquent en termes de saut de dualité.

1. INTRODUCTION

Considérons le système d'inégalités linéaires en variables 0-1 :

$$\sum_{j=1}^{n} a_{ij}x_j \leq b_i \qquad i=1,2,\ldots,m \qquad (1)$$

où : - $A = (a_{ij})$ $1\leq i\leq m$, $1\leq j\leq n$ est une matrice m x n à coefficients réels,

- $b\in R^m$

- $x\in\{0,1\}^n$

Sous l'hypothèse que le système (1) admet une solution on définit dans ce papier une mesure de la difficulté à déterminer si une variable prend une valeur fixe dans toutes les solutions du système (1). Nous appellerons permanent l'ensemble des variables à valeur fixe et satisfaisant (1), généralisant ainsi la définition de permanent défini pour les problèmes de recouvrement dans les graphes (cf. Hammer, Hansen et Simeone, 1982). On rappelle que l'identification de tous les éléments du permanent est un problème NP-complet (Valiant, 1976).

Pour identifier les éléments du permanent de (1), on utilisera une méthode de résolution basée sur l'extraction de relations logiques à partir de contraintes composites (Jaumard et Minoux, 1984). Après avoir rappelé les principes de cette technique dans le paragraphe suivant, nous montrerons qu'elle permet d'autant mieux de déterminer qu'une variable x_k a une valeur fixe que les problèmes mathématiques (P_k) et (Q_k) correspondant respectivement à : Maximiser x_k et : Maximiser $y_k = \bar{x}_k$ sur un ensemble de contraintes que nous préciserons ultérieurement, ont un faible saut de dualité.

Nous présenterons ensuite une illustration de ce résultat sur une application concernant les problèmes de confidentialité dans les votes où il s'agit de donner le maximum d'informations tout en s'assurant qu'aucun

élément du vote ne peut être déterminé, soit encore que le permanent d'un système tel que (1) est vide. Nous montrerons en particulier sur cet exemple comment une simple reformulation du problème peut permettre de :

i) faire décroître les sauts de dualité des problèmes (P_k) et (Q_k),

ii) calculer aisément le permanent du système d'inégalités considéré à l'aide des techniques d'extraction de relations logiques sans avoir recours aux méthodes beaucoup plus lourdes d'énumération implicite.

2. EXTRACTION DE RELATIONS LOGIQUES DANS UN SYSTÈME LINÉAIRE EN VARIABLES 0-1

Pour résoudre les problèmes de programmation en variables 0-1, on s'aperçoit qu'il est souvent intéressant, avant d'appliquer un algorithme général d'énumération implicite, de chercher à extraire les informations pouvant se mettre sous la forme d'un ensemble de relations logiques entre les variables :

- relations unaires (une variable est fixée à 1 ou à 0),
- relations binaires ($xy=0$, $\bar{x}y=0$, $x\bar{y}=0$ ou $\bar{x}\bar{y}=0$ avec $\bar{x}=1-x$ et $\bar{y}=1-y$),
- relations ternaires ou d'ordre plus élevé ($xyz = 0$, $\bar{x}y\bar{z}\bar{t} = 0$,...).

Ces relations peuvent être exploitées soit pour montrer que le problème n'a pas de solution, soit pour réduire le problème (éliminer, identifier ou fixer un certain nombre de variables) et faciliter sa résolution ultérieure (cf. Hammer et Nguyen, 1972; Breu et Burdet, 1974; Hansen, 1974; Johnson, Kostreva et Suhl, 1985; Jaumard, 1986; Hansen et Jaumard, 1986).

Il existe des techniques simples et efficaces pour extraire des conclusions logiques de chacune des contraintes du problème prise individuellement. Cependant sur certains problèmes, le fait de considérer les contraintes une par une limite considérablement la quantité d'information

susceptible d'être extraite de l'ensemble des contraintes. Généralisant la technique dite d'"appariement des contraintes" de Hammer, Padberg et Peled (1975), Jaumard et Minoux (1984) (voir aussi Charnes, Granot et Granot, 1975) ont proposé une nouvelle méthode d'extraction de relations logiques basée sur la construction d'une contrainte composite réunissant toutes les contraintes du problème.

Notons ici que des travaux ont également été menés par Chvatal et Hammer (1977) pour déterminer l'existence d'une contrainte unique équivalente (en termes d'ensemble de solutions) à un système d'inégalités linéaires en variables 0-1, ce en généralisant les résultats de Bradley (1971) et de Rosenberg (1974) obtenus pour un système d'égalités linéaires en variables 0-1. La conclusion de leurs travaux semble montrer que, même lorsqu'une telle contrainte existe, il est difficile de l'obtenir. A l'opposé, la contrainte composite que nous suggérons d'utiliser est facile à déterminer mais n'est pas équivalente au système d'inégalités (1).

Nous rappellons dans la suite de ce paragraphe le principe d'extraction de relations logiques sur une contrainte composite pour un système d'inégalités linéaires en variables 0-1 tel que le système (1).

On se ramène tout d'abord au cas d'un système d'égalités en associant une variable d'écart x_{n+i} à chaque inégalité i,(i=1,2,...,m). On calcule une borne supérieure u_i pour chacune des variables d'écart. Une valeur possible est $u_i = b_i - \sum_{j=1}^{n} \min(0, a_{ij})$, d'autres valeurs plus fines peuvent être calculées en résolvant des problèmes de sacs de campeur, cf. Hammer, Padberg et Peled (1975). On obtient alors le système suivant :

$$\begin{cases} \sum_{j=1}^{n} a_{ij}x_j + x_{n+i} = b_i & i=1,2,\ldots,m \\ 0 \leq x_{n+i} \leq u_i & i=1,2,\ldots,m \\ x_j \in \{0,1\} & j=1,2,\ldots,n \end{cases} \qquad (2)$$

où les coefficients a_{ij} (i=1,2,...,m, j=1,2,...,n) et b_i (i=1,2,...,m) sont des réels quelconques (pas nécessairement non négatifs).

Notons t le vecteur de $\mathbb{R}^{n+m}$ tel que :

$$\begin{cases} 1 \leq j \leq n & t_j = 1 \\ n+1 \leq j \leq n+m & t_j = u_{j-n} \end{cases}$$

et redéfinissons la matrice A comme une matrice m x (n+m) telle que pour $1 \leq i \leq m$, et $n+1 \leq j \leq n+m$

$$a_{ij} = \begin{cases} 1 & \text{si } i = j-n \\ 0 & \text{si } i \neq j-n \end{cases}$$

Le système (2) se réécrit alors :

$$\begin{cases} \sum_{j=1}^{n+m} a_{ij} x_j = b_i & i=1,2,...,m \\ x_j \in \{0,1\} & j=1,2,...,n \\ 0 \leq x_j \leq t_j & j=n+1,...,n+m \end{cases} \qquad (3)$$

En attribuant aux différentes contraintes de (3) des poids λ_1, λ_2, ..., λ_m (de signes quelconques) on déduit la contrainte composite :

$$\sum_{j=1}^{n+m} \left(\sum_{i=1}^{m} \lambda_i a_{ij} \right) x_j = \sum_{i=1}^{m} \lambda_i b_i \qquad (4)$$

En utilisant la notation formelle définie par :

$$x_j^{\alpha_j} = \begin{cases} x_j & \text{si } \alpha_j = 1 \\ t_j - x_j & \text{si } \alpha_j = 0 \end{cases}$$

et en exprimant en fonction de $x_j^0 = t_j - x_j$ les termes à coefficients négatifs de (4) on obtient l'équation à coefficients positifs suivante :

$$\sum_{j=1}^{n+m} \left| \sum_{i=1}^{m} \lambda_i a_{ij} \right| x_j^{\alpha_j} = \sum_{i=1}^{m} \lambda_i b_i - \sum_{j=1}^{n+m} t_j \min \left\{ 0, \sum_{i=1}^{m} \lambda_i a_{ij} \right\} \qquad (5)$$

Définissons les fonctions A_j, (j=1,2,...,n+m) par

$$A_j(\lambda) = \sum_{i=1}^{m} \lambda_i \, a_{ij} \quad ,$$

la fonction G par

$$G(\lambda) = \sum_{i=1}^{m} \lambda_i \, b_i - \sum_{j=1}^{n+m} t_j \min \{0, A_j(\lambda)\}$$

et, pour tout $S \subseteq \{1,2,\ldots,n\}$, la fonction F_S par :

$$F_S = G(\lambda) - \sum_{j \in S} \left| A_j(\lambda) \right|$$

a partir de quoi on obtient :

Propriété 1 : S'il existe $\lambda = (\lambda_i) \in \mathbb{R}^m$ tel que $G(\lambda) < 0$ alors le système (1) n'a pas de solution.

Propriété 2 : S'il existe $\lambda = (\lambda_i)$ $i=1,2,\ldots,m \in \mathbb{R}^m$ tel que $F_S(\lambda) < 0$, alors pour tout x solution de (1) : $\prod_{j \in S} x^{\alpha_j} = 0$.

On démontre par ailleurs (Jaumard et Minoux, 1984) que pour déterminer s'il existe un tel vecteur λ, il suffit d'évaluer la fonction F_S en un nombre fini de vecteurs correspondant aux points et aux rayons extrémaux d'un certain système d'équations linéaires.

Dans le cas général, les fonctions F_S et G sont des fonctions continues et non différentiables et la fonction G est convexe. Dans le cas particulier où S est réduit à un seul élément k, la fonction $F_k = F_{\{k\}}$ correspondante est égale au minimum de deux fonctions convexes :

$$\forall \quad \lambda \in \mathbb{R}^m \qquad (F_k(\lambda) = \min (F_k^+(\lambda), F_k^-(\lambda))$$

où :

$$\begin{cases} F_k^+(\lambda) = G(\lambda) - A_k(\lambda) \\ F_k^-(\lambda) = G(\lambda) + A_k(\lambda) \end{cases}$$

avec F_k^+ et F_k^- convexes.

On montre aisément que pour $|S| \neq 1$ la fonction F_S s'exprime comme le minimum de $2^{|S|}$ fonctions convexes. Pour $|S| = 2$ la dérivation de conclusions logiques (fixations de variables, identifications ou contradiction) à partir de relations logiques du type $\prod_{j \in S} x^{\alpha_j} = 0$ est encore un problème polynomial facile à résoudre (cf. Hansen, Jaumard et Minoux, 1985) alors que pour $|S| > 3$ le problème devient NP-complet (Cook, 1971). Cependant, compte tenu de l'augmentation du nombre des fonctions à étudier (déjà 4 pour $|S| = 2$), on se limite dans la suite de cette étude au cas $|S| = 1$.

Les techniques d'optimisation non différentiables, en particulier les algorithmes de sous-gradients, permettent d'ajuster itérativement les multiplicateurs λ des fonction $F_k^+(\lambda)$ et $F_k^-(\lambda)$ pour déterminer si les propriétés 1 ou 2 sont vérifiées.

Propriété 3 : Si le système (1) admet une solution et s'il existe $\lambda \in \mathbb{R}^m$ tel que $F_k(\lambda) < 0$ alors : $A_k(\lambda) \neq 0$ et

si $A_k(\lambda) > 0$ alors : $x_k = 0$ et $F_k(\lambda) = F_k^+(\lambda)$

si $A_k(\lambda) < 0$ alors : $x_k = 1$ et $F_k(\lambda) = F_k^-(\lambda)$.

Propriété 4 : Si le système (1) admet une solution et s'il existe un vecteur $\tilde{\lambda} \in \mathbb{R}^m$, tel que :

i) $F_k^+(\tilde{\lambda}) < 0$ alors $F_k^-(\tilde{\lambda}) > 0$

ii) $F_k^-(\tilde{\lambda}) < 0$ alors $F_k^+(\tilde{\lambda}) > 0$

Démonstration : Pour tout $\lambda \in \mathbb{R}^m$ $F_k^+(\lambda) + F_k^-(\lambda) = 2G(\lambda) > 0$ puisque l'on suppose que le système (1) admet une solution.

D'où, s'il existe $\tilde{\lambda} \in \mathbb{R}^m$ tel que :

i) $F_k^+(\tilde{\lambda}) < 0$ alors $F_k^-(\tilde{\lambda}) = 2G(\lambda) - F_k^+(\tilde{\lambda}) > 0$

ii) $F_k^-(\tilde{\lambda}) < 0$ alors $F_k^+(\tilde{\lambda}) = 2G(\lambda) - F_k^-(\tilde{\lambda}) > 0$.

Q.E.D.

3. LIENS ENTRE FIXATIONS DE VARIABLES ET SAUT DE DUALITÉ

La méthode d'extraction de relations logiques présentée à la section 2 ne permet pas toujours d'identifier toutes les variables ayant une valeur fixe dans toutes les solutions du système (1). Cette faiblesse peut être due aux limites de la méthode des contraintes composites ou à un arrêt avant un ajustement suffisant des multiplicateurs λ. Nous présentons dans cette section une caractérisation des variables qui prennent une valeur fixe dans toutes les solutions et que l'on est capable d'identifier par la méthode des contraintes composites.

Soit x_k une variable bivalente ayant une valeur fixe dans toutes les solutions du système (1). Montrons que l'existence d'un vecteur λ, $\lambda \in \mathbb{R}^m$, tel que $F_k(\lambda) < 0$ dépend du saut de dualité des programmes linéaires suivants :

$$(P_k) \begin{cases} \text{Maximiser } x_k \\ \text{sous les contraintes} \begin{cases} \sum_{j=1}^{n+m} a_{ij}x_j = b_i & i=1,2,\ldots,m \\ 0 \leq x_j \leq t_j & j=1,2,\ldots,n+m \quad j\neq k \\ 0 \leq x_k \end{cases} \end{cases}$$

dans le cas où $x_k = 0$, et

$$(Q_k) \begin{cases} \text{Maximiser } y_k = \bar{x}_k \\ \text{sous les contraintes} \begin{cases} \sum_{\substack{j=1 \\ j\neq k}}^{n+m} a_{ij}x_j - a_{ik}y_k = b_i - a_{ik} & i=1,2,\ldots,m \\ 0 \leq x_j \leq t_j & j=1,2,\ldots,n+m \quad j\neq k \\ 0 \leq \bar{x}_k \end{cases} \end{cases}$$

dans le cas où $x_k = 1$.

Théorème : Soit x_k une variable bivalente prenant la valeur 0 dans toute solution du système (1).
Il existe un vecteur λ, $\lambda \in \mathbb{R}^m$, tel que $F_k(\lambda) < 0$ si et seulement si le saut de dualité de (P_k) est strictement inférieur à 1.

Démonstration :

Soit (DP_k) le problème dual de (P_k).

$$(DP_k)\begin{cases} \text{Minimiser } \sum_{i=1}^{m} \lambda_i b_i + \sum_{\substack{j=1 \\ j\neq k}}^{m} \mu_j t_j \\ \text{sous les contraintes} \begin{cases} \sum_{i=1}^{m} \lambda_i a_{ij} + \mu_j \geq 0 & \text{pour tout } j\neq k \\ \sum_{i=1}^{m} \lambda_i a_{ik} \geq 1 \\ \mu_j \geq 0 & \text{pour tout } j\neq k \end{cases} \end{cases}$$

(DP_k) peut être simplifié en remarquant que :

$$\mu_j = \max \{0, -\sum_{i=1}^{m} \lambda_i a_{ij}\} \qquad \text{pour tout } j\neq k$$

(DP_k) se réécrit alors comme un programme mathématique avec une seule contrainte :

$$\begin{cases} \text{Minimiser } \sum_{i=1}^{m} \lambda_i b_i - \sum_{\substack{j=1 \\ j\neq k}}^{n+m} t_j \min (0, \sum_{i=1}^{m} \lambda_i a_{ij}) \\ \text{sous la contrainte : } \sum_{i=1}^{m} \lambda_i a_{ik} \geq 1 \end{cases}$$

Comme $\sum_{i=1}^{m} \lambda_i a_{ik} \geq 1$ implique $\min (0, \sum_{i=1}^{m} \lambda_i a_{ik}) = 0$, le problème se réécrit :

$$\begin{cases} \text{Minimiser } G(\lambda) \\ \text{sous la contrainte : } \sum_{i=1}^{m} \lambda_i a_{ik} \geq 1 \end{cases}$$

Soit x^* le vecteur optimal du problème (P_k), λ^* le vecteur optimal du problème (DP_k).

Condition nécessaire.

Si le saut de dualité est strictement inférieur à 1,

$$G(\lambda^*) < 1 \quad \text{avec} \quad \sum_{i=1}^{m} \lambda_i^* a_{ik} > 1$$

D'où $F_k^+(\lambda^*) = G(\lambda^*) - \sum_{i=1}^{m} \lambda_i^* a_{ik} < 0$

et $F_k(\lambda^*) = \min (F_k^+(\lambda^*), F_k^-(\lambda^*)) < 0.$

Condition suffisante.

S'il existe λ tel que $F_k(\lambda) < 0$, comme la variable x_k est fixée à 0,

$$F_k(\lambda) = F_k^+(\lambda) \quad \text{et} \quad \sum_{i=1}^{m} \lambda_i a_{ik} > 0$$

Donc $G(\lambda) - \sum_{i=1}^{m} \lambda_i a_{ik} < 0$

et $G(\lambda) < \sum_{i=1}^{m} \lambda_i a_{ik}.$

On définit $\bar{\lambda}$ tel que $\bar{\lambda}_j = \lambda_j / \sum_{i=1}^{m} \lambda_i a_{ik}$ (j=1,2,...,m). On obtient par linéarité de la fonction G que

$$G(\bar{\lambda}) < \sum_{i=1}^{m} \bar{\lambda}_i a_{ik}.$$

Comme $\sum_{i=1}^{m} \bar{\lambda}_i a_{ik} = 1$, $\bar{\lambda}$ est solution réalisable de (DP_k),

$$G(\lambda^*) \leq G(\bar{\lambda}) < \sum_{i=1}^{m} \bar{\lambda}_i a_{ik} = 1$$

et le saut de dualité est strictement inférieur à 1. Q.E.D.

Théorème 2 : Soit x_k une variable bivalente prenant la valeur 1 dans toutes les solutions de 1.

Il existe un vecteur λ, $\lambda \in \mathbb{R}^m$ tel que $F_k(\lambda) < 0$ si et seulement si le saut de dualité de Q_k est strictement inférieur à 1.

Démonstration :

Soit (DQ_k) le problème dual de (Q_k).

$$(DQ_k)\begin{cases} \text{Minimiser } \sum_{i=1}^{m} \lambda_i b_i + \sum_{\substack{j=1 \\ j\neq k}}^{n+m} \nu_j t_j - \sum_{i=1}^{m} \lambda_i a_{ik} \\ \text{sous les contraintes} \begin{cases} \sum_{i=1}^{m} \lambda_i a_{ij} + \nu_j \geq 0 & \text{pour tout } j\neq k \\ -\sum_{i=1}^{m} \lambda_i a_{ik} \geq 1 & \text{pour tout } j\neq k \\ \nu_j \geq 0 \end{cases} \end{cases}$$

dont on déduit : $\nu_j = \max\left(0, -\sum_{i=1}^{m} \lambda_j a_{ij}\right)$ pour tout $j\neq k$

(DQ_k) se réécrit comme un programme mathématique avec une seule contrainte :

$$\text{Minimiser } \sum_{i=1}^{m} \lambda_i b_i - \sum_{\substack{j=1 \\ j\neq k}}^{n+m} t_j \min\left(0, \sum_{i=1}^{m} \lambda_i a_{ij}\right) - \sum_{i=1}^{m} \lambda_i a_{ik}$$

$$\text{sous la contrainte } \sum_{i=1}^{m} \lambda_i a_{ik} \leq -1.$$

Comme $\sum_i \lambda_i a_{ik} \leq -1$ implique $\min\left(0, \sum_{i=1}^{m} \lambda_i a_{ik}\right) = \sum_{i=1}^{m} \lambda_i a_{ik}$, le problème se réécrit : $\begin{cases} \text{Minimiser } G(\lambda) \\ \text{Sous la contrainte } \sum_{i=1}^{m} \lambda_i a_{ik} \leq -1. \end{cases}$

Soit x^* le vecteur optimal du problème (Q_k), λ^* le vecteur optimal du problème (DQ_k).

Condition nécessaire.

Si le saut de dualité est strictement inférieur à 1,

$$G(\lambda^*) < 1 \quad \text{avec} \quad \sum_{i=1}^{m} \lambda_i^* a_{ik} \leq -1$$

D'où $$F_k^-(\lambda^*) = G(\lambda^*) + \sum_{i=1}^{m} \lambda_i^* a_{ik} < 0$$

et $$F_k(\lambda^*) = \min (F_k^+(\lambda^*), F_k^-(\lambda^*)) < 0$$

Condition suffisante.

S'il existe λ tel que $F_k(\lambda) < 0$, comme la variable x_k est fixée à 1,

$$F_k(\lambda) = F_k^-(\lambda) \quad \text{et} \quad \sum_{i=1}^{m} \lambda_i a_{ik} < 0$$

Donc $$G(\lambda) + \sum_{i=1}^{m} \lambda_i a_{ik} < 0$$

et $$G(\lambda) < - \sum_{i=1}^{m} \lambda_i a_{ik}.$$

On définit $\bar{\lambda}$ tel que $\bar{\lambda}_j = -\lambda_j / \sum_{i=1}^{m} \lambda_i a_{ik}$ (j=1,2,...,m). On obtient par linéarité de la fonction G que

$$G(\bar{\lambda}) < - \sum_{i=1}^{m} \bar{\lambda}_i a_{ik}$$

Comme $\sum_{i=1}^{m} \bar{\lambda}_i a_{ik} = -1$, $\bar{\lambda}$ est solution réalisable de (DQ_k)

$$G(\lambda^*) \leq G(\bar{\lambda}) < - \sum_{i=1}^{m} \bar{\lambda}_i a_{ik} = 1$$

et le saut de dualité est strictement inférieur à 1. Q.E.D.

Il existe des situations où les problèmes (P_k) et (Q_k) ont des sauts de dualité supérieurs ou égaux à 1, alors que la variable x_k a une valeur fixe dans toutes les solutions entières du système (1). Le problème suivant en est un exemple.

Considérons le système d'égalités :

$$\begin{cases} x_1 + x_2 = 1 \\ x_2 + x_3 = 1 \\ x_1 + x_3 + x_4 = 1 \\ x_4 + x_5 = 1 \end{cases} \qquad x_i \in \{0,1\} \ (i=1,2,\ldots,5) \quad (6)$$

On vérifie aisément que le système (6) admet une solution unique (0,1,0,1,0).

Montrons que l'on ne peut retrouver ce résultat à partir de la résolution des problèmes (P_k) et (Q_k) $(k=1,2,\ldots,5)$. Examinons tout d'abord la variable x_5 et les problèmes (P_5) et (Q_5) :

(P_5) Maximiser x_5

sous les contraintes

$$\begin{cases} x_1 + x_2 = 1 \\ x_2 + x_3 = 1 \\ x_1 + x_3 + x_4 = 1 \\ x_4 + x_5 = 1 \\ 0 \leq x_i \leq 1 \quad i=1,2,3,4 \\ 0 \leq x_5 \end{cases}$$

(Q_5) Maximiser $y_5 = \bar{x}_5$

sous les contraintes

$$\begin{cases} x_1 + x_2 = 1 \\ x_2 + x_3 = 1 \\ x_1 + x_3 + x_4 = 1 \\ x_4 + y_5 = 0 \\ 0 \leq x_i \leq 1 \quad i=1,2,3,4 \\ 0 \leq \bar{x}_5 \end{cases}$$

L'optimum de (P_5) est égal à $z_5^* = 1$ avec une solution optimale égale à $(\frac{1}{2},\frac{1}{2},\frac{1}{2},0,1)$, ce qui ne permet pas de conclure à l'existence d'une valeur unique (égale à zéro) de x_5 dans toute solution de (6). Il en est de même avec le problème (Q_5) dont l'optimum est égal à $\bar{z}_5 = 1$ et la solution optimale égale à (0,1,0,1,1). Remarquons d'autre part que, si on examine la variable x_4, on obtient que $\bar{z}_4 = 0$ et on conclut que $x_4 = 1$

dans toute solution entière de (6). Si on réexamine par la suite x_5 on peut conclure que $x_5 = 0$, de même, en examinant les autres variables, on obtient que (0,1,0,1,0) est la seule solution entière du système (6).

Cet exemple montre qu'en réalisant la fixation d'autres variables il est parfois possible d'abaisser à une valeur strictement inférieure à 1 le saut de dualité initialement supérieur à 1 des problèmes (P_k) ou (Q_k).

4. ÉTUDE D'UNE EXTENSION DU PROBLÈME D'AFFECTATION GÉNÉRALISÉE

Nous nous proposons d'illustrer les résultats théoriques des paragraphes précédents sur une classe de problèmes de type affectation généralisée, intervenant dans les problèmes de confidentialité de vote.

On s'intérese à un système de vote défini par un groupe de N_a actionnaires j (chacun pourvu d'un poids p_j) qui élisent une personne parmi un groupe de N_c candidats. On suppose qu'un actionnaire ne peut voter que pour un seul candidat et que, étant donné un candidat i, il y a au moins un actionnaire j qui a voté pour i. À l'issue du vote, chacun des candidats a recueilli un poids P_i et le candidat qui a le plus grand poids est élu. Supposant que l'on connaît : (i) le nombre exact n_j d'actionnaires ayant voté pour un candidat i donné et, (ii) un encadrement du poids P_i recueilli par chacun des candidats en fonction d'un paramètre de précision ε $(P_i^-(\varepsilon) \leq P_i \leq P_i^+(\varepsilon))$, on se pose la question de savoir si ces informations, (i) et (ii), peuvent permettre de déterminer certains éléments du vote et si oui lesquels. Définissant les variables bivalentes x_{ij}, $(i=1,2,\ldots,N_c,\ j=1,2,\ldots,N_a)$ par

$$\begin{cases} x_{ij} = 1 & \text{si l'actionnaire j a voté pour le cardidat i,} \\ x_{ij} = 0 & \text{sinon} \end{cases}$$

le vote reste secret si le permanent du système (S_ε) ci-dessous est vide, i.e. aucune variable n'a une valeur fixe dans toute solution de (S_ε).

$$(S_\varepsilon)\begin{cases} \sum_{i=1}^{N_c} x_{ij} = 1 & j=1,2,\ldots,N_a \\ P_i^-(\varepsilon) \leq \sum_{j=1}^{N_a} p_j\, x_{ij} \leq P_i^+(\varepsilon) & i=1,2,\ldots,N_c \\ \sum_{j=1}^{N_a} x_{ij} = n_i & i=1,2,\ldots,N_c \\ x_{ij} \in \{0,1\} & i=1,2,\ldots,N_c,\ \ j=1,2,\ldots,N_a \end{cases}$$

Le système d'équations (S_ε) obtenu correspond à un problème fortement contraint (ce d'autant plus que ε est petit). De fait, la région réalisable en nombres réels est petite, ce qui entraîne d'importants sauts de dualité. Bien souvent, en dépit d'un faible nombre de solutions, il est difficile d'extraire de l'information.

Nous illustrons la corrélation entre le saut de dualité et la difficulté de détecter les variables à valeur fixe sur l'un des problèmes réels qui nous fut fourni aved $N_c = 6$ et $N_a = 26$, soit un système (S_ε) de 156 variables et 44 contraintes. On considère de plus l'instance du problème tel que $\varepsilon = 0{,}0005$, $P_i^-(\varepsilon) = P_i - \varepsilon$ et $P_i^+(\varepsilon) = P_i + \varepsilon$ $(i=1,2,\ldots,N_c)$.

Utilisant une méthode d'énumération explicite, on montre que ce problème admet 9 solutions et 98 variables à valeur fixe (cf. tableau 1 ci-dessous).

		actionnaires																								
	i/j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
candidats	1	-	0	0	0	-	0	0	1	0	0	0	-	0	0	0	0	0	0	0	0	0	0	0	0	0	-
	2	-	0	-	0	0	0	-	0	-	0	0	-	-	0	-	-	-	0	-	0	0	0	-	0	0	0
	3	-	-	-	0	0	-	-	0	0	0	-	0	0	0	-	0	0	-	0	0	-	-	0	0	0	0
	4	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
	5	-	-	-	0	-	-	0	0	-	0	0	-	-	0	-	0	-	-	0	-	-	0	-	1	0	-
	6	-	0	-	0	0	-	-	0	-	1	-	-	-	0	0	-	-	-	-	-	-	-	-	0	0	-

Tableau 1 - Permanent du système (S_ε), $\varepsilon = 0{,}0005$

Utilisant un algorithme de sous-gradients (Shor, 1968), on a ensuite calculé le minimum de chacune des fonctions F_k, ($k=1,2,\ldots, N_a x N_c=156$) à l'intérieur d'une procédure itérative. Dès qu'une variable x_k est déclarée appartenir au permanent (S_ε), i.e. il existe un vecteur λ tel que $F_k(\lambda)< 0$, le système (S_ε) est réduit. Il peut ainsi arriver qu'au premier passage on ne détecte pas qu'une variable x_k donnée appartienne au permanent, mais que, lors d'un second passage, après avoir fixé d'autres variables, on détermine un vecteur λ tel que $F_k(\lambda)<0$.

Après avoir appliqué une telle procédure au système (S_ε), ε=0,0005, on a obtenu les fixations de variables données dans le tableau 2 ci-dessous.

		actionnaires																									
	i/j	1	2	3	4	5	6	7	8	9	10	11	12	14	14	15	16	17	18	19	20	21	22	23	24	25	26
candidats	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	-	-	-	-	-	-	-	0	0	-
	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0	-
	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0	-
	4	-	-	-	-	-	-	0	-	0	-	-	0	0	-	-	0	0	-	-	0	-	-	0	0	1	-
	5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	0	-
	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0	-

Tableau 2 - Ensemble des variables fixées grâce aux fonctions F_k

On constate que seulement 20 variables au lieu de 98 ont pu être fixées. On a vérifié que pour les 78 variables que l'on n'a pas réussi à fixer, le saut de dualité des problèmes (P_k) et (Q_k) est supérieur ou égal à 1. Ceci montre que quand les variables n'ont pu être fixées par l'algorithme, c'est dû aux limites imposées par les théorèmes 1 et 2 et non à un arrêt prématuré dû à l'ajustement des λ avant d'atteindre l'optimalité.

Nous avons par la suite étudié l'effet du paramètre ε sur le saut de dualité des problèmes (P_k) et (Q_k) et sur le nombre de variables pouvant être fixées. En diminuant ε à partir de ε=0,0005 les sauts de dualité

ne diminuent pratiquement pas et le nombre de variables pouvant être fixées ne change pas. En augmentant ε, et surtout pour $\varepsilon = 0,5$, les sauts de dualité augmentent et le nombre de variables pouvant être fixées est réduit. Le tableau 3 présente l'évolution du saut de dualité de P_k pour quatre variables typiques.

ε	$P_{3,16}$	$P_{6,24}$	$P_{1,20}$	$P_{3,18}$
0,00005	0,961	0,863	1,000	1,000
0,00050	0,961	0,863	1,000	1,000
0,00500	0,962	0,864	1,000	1,000
0,05000	0,973	0,877	1,000	1,000
0,50000	1,000	1,000	1,000	1,000

Tableau 3 : Saut de dualité en fonction de ε

5. ÉTUDE D'UNE REFORMULATION DU PROBLÈME FACILITANT L'EXTRACTION DE RELATIONS LOGIQUES

On présente dans cette section une reformulation du système (S_ε) en problème de partitionnement permettant de déterminer facilement le permanent du système (S_ε).

On rappelle ci-dessous une méthode classique (cf. Geoffrion, 1974; Fischer, 1981) de transformation d'un problème du type affectation généralisée en un problème de partitionnement.

Considérons les sous-systèmes $(S_i)_\varepsilon$, $(i=1,2,\ldots,N_c)$ des systèmes (S_ε) suivants :

$$(S_i)_\varepsilon \begin{cases} p_i^-(\varepsilon) \leq \sum_{j=1}^{N_a} p_j x_{ij} \leq p_i^+(\varepsilon) \\ \sum_{j=1}^{N_a} x_{ij} = n_i \\ x_{ij} \in \{0,1\} \qquad j=1,2,\ldots,N_a \end{cases}$$

Calculons les ensembles E_i de solutions entières de chacun des systèmes d'équations $(S_i)_\varepsilon$ et définissons la matrice A^i de dimension $N_a \times |E_i|$ telle que chaque vecteur-colonne de A^i correspond à une solution réalisable de E_i.

Considérons la matrice A suivante :

	A^1	A^2	...	A^{N_C}
A =	11... 1	11... 1	...	11... 1

Notons $N = \sum_{i=1}^{N_C} |E_i|$.

Le système d'équations de type partitionnement :

$$(R_\varepsilon) \begin{cases} Ay = 1 \\ y \in \{0,1\}^N \end{cases}$$

où A est une matrice de dimension $(N_C + N_a) \times N$

est équivalent au système d'équations du type affectation généralisée (S_ε) au sens où il existe une relation biunivoque entre l'ensemble des solutions de (R_ε) et l'ensemble des solutions de (S_ε). En effet, une solution x du problème (S_ε) se définit à partir d'une solution y de R_ε :

$$x_{ij} = \sum_{\ell \in E_i} y_\ell \, a_{j\ell} \qquad i=1,2,\ldots,N_C,\ j=1,2,\ldots,N_a \qquad (7)$$

De même, une solution y du problème (R_ε) s'obtient à partir d'une solution x de (S_ε). Soit i tel que ℓ soit une colonne de la sous-matrice A^i, alors on obtient :

$$y_\ell = \sum_{j=1}^{N_a} x_{ij}\, a_{j\ell} \qquad (8)$$

Cherchant à déterminer les solutions du système (S_ε) on pourra considérer le problème suivant :

$$(T_\varepsilon) \begin{cases} A_y = 1 \\ y \in \{0,1\}^N \\ x_{ij} = \sum_{\ell \in E_i} y_\ell\, a_{j\ell} \qquad i=1,2,\ldots,N_c, \quad j=1,2,\ldots,N_a \end{cases}$$

Nous avons expérimenté la méthode d'extraction de relations unaires, i.e. la détermination des variables à valeur fixe, sur chacun des problèmes (R_ε) et (T_ε) pour différentes valeurs de ε. Parallèlement, on utilise une méthode d'énumération pour déterminer le permanent exact de chacun de ces problèmes et également des systèmes (S_ε) correspondant. Les résultats obtenus sont résumés dans le tableau 4 ci-dessous. Les fonctions $P_i^-(\varepsilon)$ et $P_i^+(\varepsilon)$ $(i=1,2,\ldots,N_c)$ ont été définies ainsi :

$$P_i^-(\varepsilon) = \left\lceil \frac{P_i + \varepsilon}{2\varepsilon} \right\rceil \times 2\varepsilon - \varepsilon$$

$$P_i^+(\varepsilon) = \left\lceil \frac{P_i + \varepsilon}{2\varepsilon} \right\rceil \times 2\varepsilon + \varepsilon \,.$$

Le symbole $\lceil x \rceil$ désigne le plus petit entier supérieur ou égal à x. Dans les cas où $\varepsilon = 0{,}5 \times 10^{-\alpha}$, $\left\lceil \frac{P_i + \varepsilon}{2\varepsilon} \right\rceil \times 2\varepsilon$ est la valeur du vote du candidat i arrondi à α décimales.

ε	N	NS	N_0	N_1	t_R	t_T	V_0	V_1
0,00050	19	1	13	6	100	100	130	26
0,00175	62	1	56	6	100	100	130	26
0,00200	71	3	60	2	100	100	117	14
0,00250	78	2	67	1	100	100	114	10
0,00400	134	9	106	1	100	100	88	5
0,00500	168	17	143	1	100	100	93	5
0,00700	214	47	141	1	100	100	68	4
0,00800	241	27	189	1	100	100	68	4
0,01000	306	16	271	1	100	100	82	4

Tableau 4 : Résultats expérimentaux de détermination du permament sur les problèmes (R_ε) et (T_ε)

ε = valeur du paramètre de précision

N = nombre de variables du problème de partitionnement R_ε

NS = nombre de solutions du problème de partitionnement R_ε

N_0 = nombre de variables de valeur fixe 0 dans R_ε

N_1 = nombre de variables de valeur fixe 1 dans R_ε

t_R = pourcentage de variables du permanent de R_ε obtenues par la méthode d'extraction des relations unaires.

t_T = pourcentage de variables du permanent de T_ε obtenues par la méthode d'extraction des relations unaires.

V_0 = nombre de variables fixées à 0 dans le permanent de S_ε

V_1 = nombre de variables fixées à 1 dans le permanent de S_ε

On remarque que la méthode d'extraction de relations unaires permet de déterminer le permanent exact des différents problèmes (R_ε). Par suite, on est alors capable, à partir des problèmes (T_ε), de déterminer le permanent exact des problèmes (S_ε). Ceci signifie que le saut de dualité des différents problèmes (P_k) ou (Q_k) correspondant à des variables du permanent est strictement inférieur à 1, sinon sur le problème initial, du moins après avoir simplifié le problème suite à la détermination d'une partie du permanent.

Les deux dernières colonnes du tableau indiquent le nombre de variables fixées à 0 et à 1 dans le permanent de (S_ε). Ces nombres diminuent généralement quand ε augmente. Ainsi, le vote peut être complètement décodé pour ε=0,0005 et 0,00175, et le secret augmente avec ε. Toutefois, plus de la moitié des variables sont encore fixes et identifiables pour ε=0,01.

Notons également que les temps de calcul obtenus sur un CYBER sont de l'ordre de la minute pour l'ensemble des problèmes traités ($N < 100$) et semblent comparables pour les deux méthodes utilisées. Nous ne les avons pas indiqués de façon précise dans le tableau 4 en raison du caractère largement expérimental des algorithmes utilisés : l'objectif de la présente étude n'était pas une étude comparative en termes de temps de calcul de différentes approches mais une illustration précise du lien entre saut de dualité et difficulté de résolution d'un problème fortement contraint. En particulier, l'algorithme d'extractions de relations unaires devrait être facilement améliorable, à la fois en exploitant le caractère creux de la matrice des contraintes après avoir fixé certaines variables et à la fois en définissant un critère sur l'ordre d'examen des variables.

6. CONCLUSION

Les théorèmes de la section 3 établissent des conditions nécessaires et suffisantes pour que la méthode d'extraction de relations logiques identifie qu'une variable a une valeur fixe dans toutes les solutions. L'exemple du décodage du vote illustre que ces conditions portant sur le saut de dualité peuvent être satisfaites ou pas suivant le choix de la formulation du problème.

RÉFÉRENCES

BRADLEY, G.H., "Transformation of Integer Programs to Knapsack Problems", Discrete Math. 1 (1971) 29-45.

BREU, R. et BURDET, C.A., "Branch and Bound Experiments in Zero-one Programming", Mathematical Programming Study 2 (1974) 1-50.

CHARNES, A., GRANOT, D. et GRANOT, F., "On Improving Bounds for Variables in Linear Integer Programs by Surrogate Constraints", INFOR 13, 3 (1975) 260-269.

CHVATAL, V. et HAMMER, P.L., "Aggregation of Inequalities in Integer Programming", Annals of Discrete Mathematics 1 (1977) 145-162.

COOK, S.A. "The Complexity of Theorem Proving Procedures", Proceedings of the Third Annual Symposium on Theory of Computing (1971) 151-158.

FISCHER, M.L., "The Lagrangian Relaxation Method for Solving Integer Programming Problems", Management Science 27 (1981) 1-18.

GEOFFRION, A.M., "Lagrangian Relaxation and its Uses in Linear Programming", Mathematical Programming Study 2 (1974) 82-114.

GOFFIN, J.L., "On Convergence Rates of Subgradient Optimization Methods", Mathematical Programming 13 (1977) 329-347.

HAMMER, P.L., PADBERG, M.W. et PELED, U.N., "Constraint Pairing in Integer Programming", Infor 13,1 (1975) 68-81.

HAMMER, P.L. et NGUYEN, S., "A Partial Order on the Solution Space of Bivalent Programs, APOSS", CRM 163, Université de Montréal (1972).

HAMMER, P.L., HANSEN, P. et SIMEONE, B., "Vertices Belonging to all or to no Maximum Stable Sets of a Graph", SIAM Journal of Algebraic and Discrete Methods 3 (1982) 511-522.

HANSEN, P., "Programmes mathématiques en variables 0-1", thèse d'aggrégation, Université Libre de Bruxelles (1974).

HANSEN, P. et JAUMARD, B., "Extraction of Logical Relations and Strong Penalties", Rutcor Research Report. (À paraître).

HANSEN, P., JAUMARD, B. et MINOUX, M., "A Linear Expected-time Algorithm for Deriving all the Logical Conclusions Implied by a Set of Boolean Inequalities", Mathematical Programming (à paraître).

JAUMARD, B., "Extraction et utilisation de relations boléennes pour la résolution des programmes linéaires en variables 0-1", thèse de doctorat, École Nationale Supérieure des Télécommunications, Paris, France (1986).

JAUMARD, B. et MINOUX, M., "Extraction of Logical Relations on Variables in Discrete Optimization - Generalization of Constraint Pairing and New Algorithms", Rapport technique, CNET/PAA/TIM/MTI/1456 (1984). Soumis pour publication.

JOHNSON, E.L., KOSTREVA, M.M. et SUHL, U.H., "Solving 0-1 Integer Programming Problems Arising from Large Scale Planning Models", Operations Research 33, 4 (1985) 803-819.

ROSENBERG, I.G., "Aggregation of Equations in Integer Programming", Discrete Math. 10 (1974) 325-341.

SHOR, N.Z., "On the Rate of Convergence of the Generalized Gradient Method", Kibernetika 4, 3 (1968) 98-99.

VALIANT, L.G., "The Complexity of Computing the Permanent", Theorical Computer Science 8 (1979) 189-221.